Method for operating a data carrier designed for executing reloadable function programs

This invention starts out from a method according to the preamble of the main claim.

Data carriers in the form of smart cards are used in an increasing variety of application areas. Especially widespread cards are ones according to the standard ISO 7810 which consist of a plastic carrier incorporating an integrated semiconductor circuit and contact means for making electric connections with a corresponding reader. It has also been proposed to make the card carrier smaller or omit it completely and instead install for example a single-chip microcontroller in watches, jewelry, garments or other articles of daily use. The term "smart card" is therefore intended to include all current and future transportable (small) objects in which a microcontroller is embedded to enable its owner or holder to perform smart card-typical interactions with corresponding, specially provided interaction stations. Typical smart card applications are the credit card, money card, health insurance card or telephone card. The term "application" refers here to the totality of all data, commands, operations, states, mechanisms and algorithms within a smart card which are necessary for operating a smart card within a system, for example a credit card payment system.

Each application usually has its own corresponding smart card, and each new application and update of an existing application likewise yield a new smart card. It is therefore fundamentally desirable to have a smart card which can be used for a plurality of applications of different service providers and operators of card systems, such as credit card organizations, banks, insurances, telephone companies, etc.

A file organization for such a smart card suitable for several applications is shown in Rankl/Effing, "Handbuch der Chipkarten," Carl Hauser Verlag, 1996, chapter 5.6. The organization structure described therein is based on ISO/IEC standard 7816-4. At the top of the file structure is a master file containing the directories of all other files present on the smart card. Subordinate to the master file are one or more dedicated files containing the file names of files combined in groups, in particular belonging to one application. Subordinate to each dedicated file are finally one or more

elementary files containing the useful data of an application. This print in addition describes the reloading of program code as technically possible but inexpedient for reasons of security. As the most promising measure for overcoming the security problems it refers to setting up a memory management unit which monitors program code to be executed as to whether it keeps to the allocated limits.

The print WO-A1-98/09257 discloses a system and method for loading applications onto a smart card which make it possible to put program and application data of further applications into a smart card in addition to the data of already loaded applications. Precautions are taken on the basis of suitable cryptographic technologies to allow verification of the authorization of the agency performing the data reloading. After the data of an additional application have entered the memory of the smart card, the authenticity of the corresponding program data is checked. Then the program data are checked with respect to their syntax and valid type limitations. If an incongruity is ascertained in one of these check steps, the additionally loaded data are discarded and deleted in the memory. The known system allows controlled reloading of applications after the card has been issued to the final user. However, it means that a card issuer issuing a smart card with available, free memory space to a service provider, for example, must already know the identity of all agencies of the service provider which are later to be entitled to offer applications to an end-user for reloading. This can be done by the card issuer certificating certain public signature keys of service providers in order to be able to do a check of the authenticity of reloaded data by depositing its own public signature key, e.g. in the ROM mask of the smart card. However, in the known system a card issuer has no possibility of checking the memory volume occupied by the service providers on a single smart card, beyond authenticity and correct syntax.

DE 197 18 115 A1 further discloses a smart card and method for loading data onto a smart card which make it possible to put card applications on a smart card after the end of the card production process. Provided on the smart card is a container storage space into which service providers can load applications of their own. In the container storage space the basic program structure of reloadable applications is

predefined; what is reloaded is only dedicated data and keys. Predefinition of the structures of loadable applications achieves a reliable separation of data of different service providers on a card. This print does not provide for the reloading of applications with unknown data structure. It does not in general describe alternatives of predefining application structures for managing the container storage space. The concept of predefining application structures cannot be used if program code of indefinite scope is to be loaded onto a card later. The solution found in DE 197 18 115 A1 is therefore unsuitable for applying complete program codes of applications later.

The invention is based on the problem of providing a method for putting an additional application on a smart card as well as a smart card which avoid the stated disadvantages of the prior art.

This problem is solved according to the invention by a method with the features stated in claim 1 and by a smart card with the features of independent claim 4. The problem is likewise solved by a method with the features stated in claim 8 and by a smart card with the features of independent claim 12. The objects of claims 1 and 4, on the one hand, and 8 and 12, on the other hand, each have independent inventive importance. The methods according to claims 1 and 8 and the objects of claims 4 and 12 can also be combined.

The inventive method according to claim 1 as well as the method according to claim 8 permit a card issuer in advantageous fashion to allow a user to put function programs into a card on his own authority later. The card issuer need no longer predefine which users or service providers are to be given permission to reload additional applications onto certain smart cards. It is instead possible to reload an application even when the smart card is already issued and in the user's possession. The method is therefore suitable in particular for realizing a contractual transfer of precisely definable rights to memory resources of smart cards to third parties by a smart card issuer.

The method ensures a high security standard. According to claim 1 this is obtained by the fact that load applications permitting reloading of application function programs can only be put on the card via a main loader interface set up on the card by

the card issuer. The main loader interface advantageously permits in particular the physical position and logical action range of a reloaded function program to be exactly defined. The creation of a possibility of reloading function programs moreover simplifies the production of the corresponding cards in advantageous fashion.

The badge system according to claim 8 offers the advantage that the card issuer can check the volume of memory space to be available to individual users for reloadable applications. The badge system in addition offers the possibility of setting up an application-related cost system. For example, it may be provided to have a user or service provider pay a share of the total costs of a smart card depending on how much of the smart card memory device he or it occupies.

Advantageous developments and expedient embodiments of the proposed method and smart card can be found in the dependent claims.

The invention will be explained in more detail in the following by an embodiment by way of example and in nonlimiting fashion with reference to the drawing, in which:

Fig. 1 shows the structure of a microprocessor smart card,

Fig. 2 shows schematically the occupancy of the memory device of a smart card with a main loader,

Fig. 3 shows the occupancy of the memory device after loading of a special loader,

Fig. 4 shows a schematic view of the hierarchical structure comprising a main loader and several special loaders.

Fig. 1 shows the typical structure of smart card 10 equipped with a microprocessor. The main element is central processor unit 20 which gives smart card 10 its functionality by executing function programs. Processor unit 20 has assigned thereto memory device 110 constructed of three memory circuits 30, 40, 50. Memory circuit 30 represents a mask-programmed read-only memory (ROM) containing in particular the operating system of central processor unit 20; memory circuit 50 represents electrically erasable read-only memory 50 (EEPROM) for receiving the program codes of function programs and data used by central processor unit 20;

memory circuit 40 represents normally volatile random access memory 40 (RAM) for use as a working memory in executing a function program. Card functionality results from the totality of the program codes or data contained in memory circuits 30, 40, 50. If this is technically necessary or expedient, memory circuits 30, 40, 50 can be used in overlapping fashion, e.g. if certain memory address areas in the EEPROM are used for program data of the operating system, or memory address areas in the ROM are occupied with application data. For this reason memory circuits 30, 40, 50 will always be understood in the following as a whole as memory device 110. For exchanging data with external devices, card 10 in addition has data interface 60 likewise connected with central processor unit 20. A typical application of card 10 shown is to execute electronic payment operations. A detailed description of the smart card shown in Fig. 1 can be found e.g. in Rankl/Effing, "Handbuch der Chipkarten," Carl Hauser Verlag, 1996, chapter 2.3.

A first embodiment of the invention is based on the concept of allowing load applications which can in turn load application function programs to be put on a card but permitting the load applications themselves to be set up solely by a special loader interface. Fig. 2 illustrates schematically the occupancy of memory device 110 of a smart card which first includes only the program code of single function program 120 defining first loader interface 120. Loader interface 120 is specially designed to reload into memory device 110 function programs which realize load applications, i.e. which in turn have load functionality and permit reloading of application function programs. Loader interface 120 is expediently part of the basic equipment of a smart card and is put on the card by the card issuer or card producer. Loader interface 120, designated main loader (HL) in the following, occupies part of the total memory area available in memory device 110. The function program realizing main loader 120 can in particular be part of the operating system of the smart card and is accordingly executed as part of the mask-programmed code in read-only memory (ROM) 30. Another part of the total memory area is initially not occupied with data and is available as free memory 130 for further function programs yet to be loaded. Management of total free memory 130 is effected first by main loader 120. In this function as a management device, main loader

120 controls in particular the loading of the program code of the first function program to be reloaded into free memory 130 and the allocation of address spaces. The byte code of the first as well as all other reloaded function programs is transmitted via data interface 60 in the form of suitable electric signals.

Main loader 120 preferably loads only those function programs into memory device 110 which fulfill defined security conditions. During loading it thus preferably checks integrity and authenticity of a load application to be loaded by checking whether the program code waiting to be loaded is present unchanged in a form approved by the producer, or whether the producer of a load application is actually authorized to put in the load application by for example having acquired a right to utilize smart card resources from the card issuer.

Fig. 3 shows the memory array from Fig. 2, whereby main loader 120 has now loaded first function program 210 realizing a load application into free memory 130. Load application 210 defines a second interface, designated special loader 210 (DL) in the following. It allows further function programs to be put into memory device 110 subsequently. However, it only has defined, unexpandable assigned address space 220 available therefor. Assigned address space 220 is allotted to special loader 210 by main loader 120 during loading of special loader 210. Said allocation transfers the management of assigned address space 220 completely to special loader 210, which has the necessary functionality as a management device for this purpose like main loader 120. Main loader 120 has no influence on, or access to, the further utilization of address space 220 assigned to special loader 210.

Main loader 120 still has management of the part of the free memory address space not occupied by being taken over by special loaders 210 and assignment of address spaces 220 and fragmented into separate sections 130a, 130b.

Special loader 210 can be loaded by the user of a card, unlike main loader 120. Special loader 210 permits, and is the precondition for, the user to load function programs realizing applications into assigned address space 220 subsequently as he chooses. The term "application" refers here to the totality of all data, commands, operations, states, mechanisms and algorithms for operating a smart card which is

application-related cost system. For example, it may be provided to have a user or service provider pay a share of the total costs of a smart card depending on how much of the smart card memory device he or it occupies.

Advantageous developments and expedient embodiments of the proposed method and smart card can be found in the dependent claims.

The invention will be explained in more detail in the following by an embodiment by way of example and in nonlimiting fashion with reference to the drawing, in which:

Fig. 1 shows the structure of a microprocessor smart card,

Fig. 2 shows schematically the occupancy of the memory device of a smart card with a main loader,

Fig. 3 shows the occupancy of the memory device after loading of a special loader,

Fig. 4 shows a schematic view of the hierarchical structure comprising a main loader and several special loaders.

Fig. 1 shows the typical structure of smart card 10 equipped with a microprocessor. The main element is central processor unit 20 which gives smart card 10 its functionality by executing function programs. Processor unit 20 has assigned thereto memory device 110 constructed of three memory circuits 30, 40, 50. Memory circuit 30 represents a mask-programmed read-only memory (ROM) containing in particular the operating system of central processor unit 20; memory circuit 50 represents electrically erasable read-only memory 50 (EEPROM) for receiving the program codes of function programs and data used by central processor unit 20; memory circuit 40 represents normally volatile random access memory 40 (RAM) for use as a working memory in executing a function program. Card functionality results from the totality of the program codes or data contained in memory circuits 30, 40, 50. If this is technically necessary or expedient, memory circuits 30, 40, 50 can be used in overlapping fashion, e.g. if certain memory address areas in the EEPROM are used for program data of the operating system, or memory address areas in the ROM are occupied with application data. For this reason memory circuits 30, 40, 50 will always

be understood in the following as a whole as memory device 110. For exchanging data with external devices, card 10 in addition has communication device 60 likewise connected with

central processor unit 20. A typical application of card 10 shown is to execute electronic payment operations. A detailed description of the smart card shown in Fig. 1 can be found e.g. in Rankl/Effing, "Handbuch der Chipkarten," Carl Hauser Verlag, 1996, chapter 2.3.

A first embodiment of the invention is based on the concept of allowing load applications which can in turn load application function programs to be put on a card but permitting the load applications themselves to be set up solely by a special loader interface. Fig. 2 illustrates schematically the occupancy of memory device 110 of a smart card which first includes only the program code of single function program 120 defining first loader interface 120. Loader interface 120 is specially designed to reload into memory device 110 function programs which realize load applications, i.e. which in turn have load functionality and permit reloading of application function programs. Loader interface 120 is expediently part of the basic equipment of a smart card and is put on the card by the card issuer or card producer. Loader interface 120, designated main loader (ML) in the following, occupies part of the total memory area available in memory device 110. The function program realizing main loader 120 can in particular be part of the operating system of the smart card and is accordingly executed as part of the mask-programmed code in read-only memory (ROM) 30. Another part of the total memory area is initially not occupied with data and is available as free memory 130 for further function programs yet to be loaded. Management of total free memory 130 is effected first by main loader 120. In this function as a management device, main loader 120 controls in particular the loading of the program code of the first function program to be reloaded into free memory 130 and the allocation of address spaces. The byte code of the first as well as all other reloaded function programs is transmitted via data interface 60 in the form of suitable electric signals.

Main loader 120 preferably loads only those function programs into memory device 110 which fulfill defined security conditions. During loading it thus preferably

checks integrity and authenticity of a load application to be loaded by checking whether the program code waiting to be loaded is present unchanged in a form approved by the producer, or whether the producer of a load application is actually authorized to put in the load application by for example having acquired a right to utilize smart card resources from the card issuer.

On the other hand, function program 330 has no possibility of access or linking with respect to function programs 311; this is blocked due to a lack of corresponding access or linking permission for function program 330, or 320, this is blocked for all external access.

Complementary to the loading of new function programs by main loader 120 or special loader 210, it is fundamentally also possible to delete function programs 210, 240, 310, 330 present in memory device 110. Entitlement to deletion is set up during loading of a function program by loader 120, 210. Deletion of special loader 210 is only possible if address space 220 assigned thereto no longer contains any function program. Main loader 120 cannot be deleted.

A measure which advantageously supports low-risk transfer of smart card memory space to third parties is the use of a badge system for carrying out the storage space allocation by main loaders 120 and/or special loaders 210a, 210b, 210c. The badges have the form of digital information. They are added to special loader 210 or a function program to be loaded and comprise in particular a statement about the size of desired assigned address space 220 or the size of address space 230 required for the function program therein. Loader 120, 210 to be used for loading a special loader or function program 230 provided with a badge must be capable of evaluating the badge. A badge system can be set up for all loaders 120, 210 of a card or only for individual ones; a hierarchical loader structure as shown in Figure 3 is not a precondition for setting it up. The badges are generated by the smart card issuer or the producer of loader 120, 210. They must also be acquired beforehand from said issuer or producer for special loader 210 to be newly loaded or a function program to be newly loaded into memory device 110. The loader producer/card issuer is in this way always informed of the occupancy of the address space assigned to its loader 120/210. By assigning only the absolutely necessary address space to special loaders or function programs to be newly loaded, it can ensure particularly memory space-saving utilization of an assigned address space by means of corresponding information on the badge.

Besides mere size information, a badge can contain further information, for example information permitting a check of the authenticity of a badge. Authenticity and forgery-proofness of a badge are further preferably ensured by cryptographic methods. The information on a badge is in this case encrypted, the badge accordingly containing for example an initialization key which allows an authorized loader to derive a key for reading the badge. Expediently, a badge further contains a cryptographically realized digital signature. To facilitate management, a badge can in addition be provided with for example the designation of a function program, an application identifier, a date or the like. It is furthermore possible to set up information which limits the usability of a function program, limiting for example the time for which an application can be used, or stating identifiers of cards which are solely entitled to use a function program.